

(19) World Intellectual Property Organization International Bureau



- 1 DEGID BERLERA DE BERLERA SERIA BARRA BERLERA BERLERA BERLERA BERLERA BERLERA BERLERA BERLERA BERLERA BERLE

(43) International Publication Date 26 February 2004 (26.02.2004)

PCT

(10) International Publication Number WO 2004/017599 A1

(51) International Patent Classification7:

H04L 29/06

(21) International Application Number:

PCT/NL2003/000585

(22) International Filing Date: 15 August 2003 (15.08.2003)

(25) Fliing Language:

Dutch

(26) Publication Language:

English

(30) Priority Data: 1021300

19 August 2002 (19.08.2002) NL

(71) Applicant (for all designated States except US): NED-ERLANDSE ORGANISATIE VOOR TOEGEPAST-NATUURWETENSCHAPPELLIK ONDERZOEK TNO [NL/NL]; Schoemakerstraat 97, NL-2628 VK Delft (NL).

(72) Inventors; and

(75) Inventors/Applicants (for US only): BIK, Albert, Louis, Caesar, Christophorus, Matthias [NL/NL]; Ooievaarstraat 209, NL-2162 XL Lisse (NL). DEGEN, Alexander, Johannes, Gerardus [NL/NL]; Velpsestraat 31, NL-2573 SB Den Haag (NL). VISSER, Coenraad, Leo, Siman [NL/NL]; Lau Mazirellaan 105, NL-2525 ZL Den Haag (NL). LACHMAN, Rajesh [NL/NL]; Beukelsdijk 168, NL-3022 DN Rotterdam (NL). NIE-LEN, Franciscus, Hendrikus [NL/NL]; Galvanistraat 70 B, NL-2517 RD Den Haag (NL).

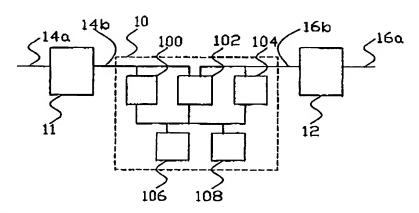
- (74) Agent: PRINS. A.W.; Nieuwe Parklaan 97, NL-2587 BN Den Haag (NL).
- (81) Designated States (national): AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK (utility model), SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

with international search report

for two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: COMPUTER NETWORK PROTECTION



(57) Abstract: The computer system comprises a local network domain of communicating computers and a connection for communication with an external network. A gate device coupled between the local network and the connection is arranged to check files sent from the local network to the connection for the presence of a security tag in the file, and to send or not send on each file to the connection depending on detection of the presence or absence of the security tag in the file.



O 2004/017599 A1

5

10

15

20

25

YPRIS

PCT/NL2003/000585 10 / 5247 25 PT01 Rec'd PCT/FTC 1:6 FEB 2005

Title: Computer network protection

The invention relates to protection against unauthorized access to (copies of) files stored in a computer network.

It is known in the present situation that in order to guarantee the confidentiality of electronic documents (also referred to below as "files") codes indicating which users are allowed to open the document are stored in a file system. Thus, for instance, this code can indicate whether only the author of the file has an access right or also a group to which this author belongs, or that everyone has an access right. When a user attempts to read such a file, the control system checks whether the respective user has an access right according to the codes for the requested file. Only if this is the case, the control system allows access.

This form of access control has the drawback that it is bound to the file system. This form of access control requires that users be divided previously into different kinds.

Another form of access control is the encryption of confidential files. Only those who have at their disposal the key required for the encryption of the file can get access in this way. The advantage over access codes is that now also all content-containing copies of the file are protected wherever they are. It is a drawback, however, that each time a key and decryption are required before access to the file is possible.

For protection against computer viruses, it is known besides to make use of a so-called firewall for the transport of files to a computer system. A firewall blocks the reception of files by a computer system when the file satisfies predetermined characteristics. A firewall, however, does not serve to keep confidential selected confidential files among files sent by the computer system.

5

10

15

20

25

30

PCT/NL2003/000585

2

It is, inter alia, an object of the invention to provide a computer system which makes it possible to selectively limit the access to files without requiring extra measures when copies are made within the computer system and without requiring encryption.

The computer system according to the invention is defined in claim 1. The invention makes use of a gate device in a communication channel between a network domain and an external connection such as a connection to the Internet. The gate device is arranged to check for the presence of a security tag all files sent to the external connection via the communication channel. Depending on the presence or absence of this security tag, the gate device limits the free sending of the file to the external connection.

In this way, a file-selective check is performed for the access possibilities to the file outside the network domain. Within the network domain, every user has access, in principle, to the file. But out of that, the access is limited. In this way, a domain specific protection is provided. In the most extreme form, the gate device blocks the sending, depending on the presence or absence of this security tag. In principle, the invention can be applied to all forms of file sending, for instance sending as part of e-mail protocols (SMTP), as part of file transfer protocols (FTP), as part of hyperlink protocols (HTTP) or any other sort of protocol.

Preferably, all communication channels of the network domain to external connections are provided with such a gate device. In one embodiment, the gate device limits free sending of files provided with such a security tag. In this way, existing or externally received files remain freely accessible, and users can themselves ask for protection.

The invention, however, is not limited to complete obstruction. In another embodiment, for instance, the gate device automatically encrypts all files provided with a security tag when these files are sent via the communication channel. In this way, protection is offered outside the network domain by means of encryption. In yet another embodiment, the

PCT/NL2003/000585

3

security tag is combined with an anti-tamper code which makes it practically impossible to remove the tag.

These and other objects and advantageous aspects of the computer system according to the invention will be described in more detail with reference to the following Figures.

Figure 1 shows a computer system
Figure 2 shows a gate device

10

15

20

25

5

Figure 1 shows a computer system with external connections 14a, 16a. The computer system comprises a domain 10 containing a number of computers 100, 102, 104, 106, 108, which are connected with each other via connections. A part of the computers 100, 102, 104, 106, 108 is connected with communication channels 14a,b, 16a,b, which run via the external connections to further computers (not shown). Located in the communication channels 14a,b, 16a,b are gate devices 11, 12. The gate devices each preferably form part of a device which also has other security tasks such as the effectuation of a firewall etc. In use, files are stored in one or more of the computers in domain 10, which files can be read via the connections from all computers in the domain. These files can be provided with security tags. In an HTML file, the security tag could, for instance, be implemented by addition of a piece of text in the form of <SECURITY> </SECURITY>, optionally supplemented with parameters. Of course, the security tag may be supplemented in all kinds of other ways, for instance by addition of other sorts of codes, or by applying a watermark in the file. Preferably, the computer is arranged to also automatically encrypt the file or the important part thereof when applying the security tag. In this way, an extra protection is realized.

5

10

15

20

25

PCT/NL2003/000585

4

When a file is sent from a computer in the domain via one of the communication channels to one of the external connections 14a, 16a, this occurs via the gate device 11 or 12. The respective gate device 11, 12 checks the file for the presence of the security tag before sending on the file to the external connection 14a, 16a. The gate device 11, 12 sends on the file only if it does not find the security tag. Besides, the gate device 11, 12 preferably stores data on the sending of the file in a log file, at least if the sending has been obstructed. This enables the system manager to check for breaches later.

Figure 2 shows an embodiment of a gate device 11 in more detail. The gate device 11 contains a first transceiver 20 for the local part of the communication channel 14b, a second transceiver 22 for the external connection 14a, a memory 24 and a tag detector 26. Transceivers 20, 22 are coupled to the memory 24. The detector 26 has an input coupled to the first transceiver 20 for the local part of the communication channel 14b and an output coupled to the second transceiver 22 for the external connection 14a.

In operation, the first transceiver 20 receives messages from the local part of the communication channel 14b and stores these messages temporarily in the memory 24. The detector 26 examines the content of the message for the presence of a file containing a security tag and sends, depending on a result of that examination, a command to the second transceiver 22. When the command purports to pass the message, the second transceiver 22 reads the message from the memory 24 and sends the message to the external connection 14a. When the message is not sent on, the message is removed from the memory 24, for instance by overwriting it with a later message without sending on the message.

The computers in the domain 10 are arranged to read or copy the respective files without a check on the security tag on all computers in the domain. In this way, it is possible to store and copy files in the domain 10 in

5

10

15

20

PCT/NL2003/000585

5

arbitrary places, but undesired or accidental sending to external connections 14a,b outside the domain is made impossible.

Without departing from the principle of the invention, all kinds of other embodiments are, of course, possible. Thus, for instance, the gate device 11, 12 may exactly not send on the file when no security tag is present. As a result, a user may deliberately choose to protect a file from sending.

As part of the protection, a tamper protection may be included such as, for instance, a code encrypted with a private key, which code can be decrypted with a public key and contains a number which is a function of the content of the file including the security tag. Before sending the file, the gate device may again calculate the code, then, on the basis of the file and compare with the code following from the file by public key decryption. In this way, it is ensured that the security tag cannot be changed. Also, the tag can be included in specific sorts of files as a watermark.

Furthermore, the gate device 11, 12, instead of not sending the file, may encrypt the file before sending it when the security tag indicates that free sending is not allowed. If desired, it may even be indicated with parameters in the security tag which action (for instance not sending or sending encryptedly) the file must undergo when passing the gate device 11, 12.

5

PCT/NL2003/000585

6

CLAIMS

- 1. A computer system, comprising
- a local network domain of communicating computers;
- a connection for communication with an external network;
- a gate device coupled between the local network and the connection, which gate device is arranged to check files sent from the local network to the connection for whether they contain a security tag, and to send or not send on each file to the connection depending on detection of the presence or

absence of the security tag in the file.

- 2. A computer system according to claim 1, wherein the gate device is arranged to block sending on of the file if the security tag is present in the file.
 - 3. A computer system according to claim 1 or 2, wherein the communicating computers are arranged to encrypt a substantial part of the file when providing the security tag.
- 4. A gate device with a coupling for connection of a local network and a connection for an external network, which gate device is arranged to check files sent from the local network to the connection for whether they contain a security tag, and to send or not send on each file to the connection depending on detection of the presence or absence of the security tag in the file.
 - 5. A method for protecting information transport from a local network to an external network, which method comprises the steps of
 - providing a security tag in selected files;
- examining files sent by a gate device of the local network to the external network for the presence of the security tags;
 - blocking or sending on those files in which a security tag is present.

PCT/NL2003/000585 10/524725

1/1

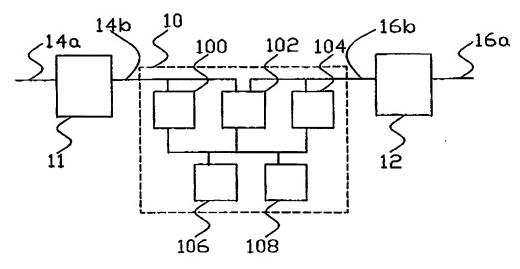
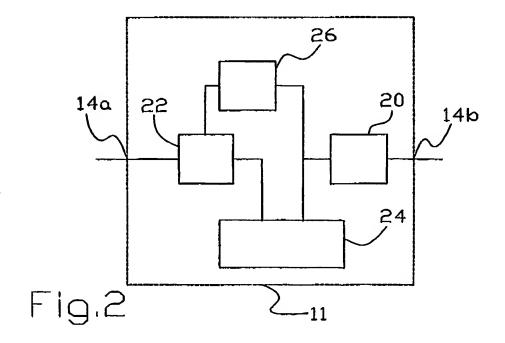


Fig. 1



Inter	pplication No
PCIZNL	u3/00585

	CAROLIDE SUB LECT MATTER		
A CLASSIFI IPC 7	CATION OF SUBJECT MATTER H04L29/06		
	International Patent Classification (IPC) or to both national classifi	cation and IPC	
B. FIELDS S			
Minimum doc	sumentation searched (classification system followed by classifica-	lion symbols)	i
IPC 7	HO4L		
	· _		
Documentation	on searched other than minimum documentation to the extent that	I such documents are included in the fields se	arched
er	ata base consulted during the international search (name of data	base and, where practical, search terms used)	
EPO-Int	cernaı		
C. DOCUME	ENTS CONSIDERED TO BE RELEVANT		Relevant to claim No.
Category "	Citation of document, with indication, where appropriate, of the	relevant passages	Halavan in ciami i.jo.
			1.6
χ	US 2002/016922 A1 (MURRAY ARNOL	D E ET AL)	1-5
	l 7 February 2002 (2002-02-07)		
	paragraph '0007!; claims 1,2		
х	US 2002/112015 A1 (HAYNES THOMA	AS RICHARD)	1-7
^	15 August 2002 (2002-08-15)		
Ì	paragraph '0014! - paragraph '	10018!	<u> </u>
Ì		•	
1	1		
ł			
į			
1			
į.			
Fu	rther documents are listed in the continuation of box C.	Patent family members are liste	d in annex.
			A
1	categories of cited documents:	"I" later document published after the in or priority date and not in conflict wi	
"A" docur	ment defining the general state of the an which is not sidered to be of particular relevance	cited to understand the principle of the invention	nedly underlying the
'E' earlie	ir document but published on or after the international	"X" document of particular relevance; the cannot be considered novel or cannot be considered nov	
44.0 -	g date ment which may throw doubts on priority claim(s) or	involve an inventive step when the	COCOURING IS ISTUDIA STOLE
which	ch is cled to establish the publication date of allotted lion or other special reason (as specified)	 Yournest of particular relevance; the cannot be considered to involve an document is combined with one or 	more other such docu-
O. docn	iment referring to an oral disclosure, use, exhibition or er means	ments, such combination being out	tous to a person skilled
.b. docn	ment published prior to the international filing date but	in the art. •&• document member of the same pate	nt family
	r then the priority date ctalmed	Date of mailing of the international	
Uate of th	ne actual completion of the international search		
	3 November 2003	10/11/2003	
Alessa si		Authorized officer	
Name an	nd mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2		
1	NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.	Veen, G	
	Fax: (+31-70) 340-3016		

INTERNATION SEARCH REPORT

Inter pplication No PCT/NL U3/00585

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
US 2002016922	A1	07-02-2002	AU TW WO	4721301 A 533723 B 0163387 A	03-09-2001 21-05-2003 30-08-2001
US 2002112015	A1	15-08-2002	US U\$	6574671 B 2002194284 A	03-06-2003 19-12-2002

Form PCT/ISA/210 (patent family annex) (July 1692)

INTERNATIONAL SEARCH REPORT

Property Description No. Property U3/00585

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 H04L29/06						
According to	o International Patent Classification (IPC) or to both national classifica	tion and IPC				
B. FIELDS	SEARCHED					
Minimum do	ocumentation searched (classification system followed by classification HO4L	n symbols)				
Documenta	tion searched other than minimum documentation to the extent that so	ich documents are included in the fields se	arched			
Electronic d	lata base consulted during the international search (name of data bas	e and, where practical, search terms used)			
EPO-In	ternal					
C. DOCUM	ENTS CONSIDERED TO BE RELEVANT					
Category °	Citation of document, with indication, where appropriate, of the rele	evant passages	Relevant to claim No.			
х	US 2002/016922 A1 (MURRAY ARNOLD 7 February 2002 (2002-02-07) paragraph '0007!; claims 1,2	1-5				
х	US 2002/112015 A1 (HAYNES THOMAS RICHARD) 15 August 2002 (2002-08-15) paragraph '0014! - paragraph '0018!					
Fur	ther documents are listed in the continuation of box C.	χ Patent family members are listed	In annex.			
"A" docum	° Special categories of cited documents: "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the					
considered to be of particular relevance invention "E" earlier document but published on or after the international "X" document of particular relevance; the claimed invention						
tiling date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the						
O document referring to an oral disclosure, use, exhibition or other means *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but *Cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.						
later than the priority date claimed "&" document member of the same patent family						
	a actual completion of the international search November 2003	Date of mailing of the International se $10/11/2003$	аки төрөп			
Name and	mailing address of the ISA	Authorized officer				
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016 Veen, G						

INTERNATIONAL SEARCH REPORT

Post U3/00585

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
US 2002016922	A1	07-02-2002	AU TW WO	4721301 A 533723 B 0163387 A2	03-09-2001 21-05-2003 30-08-2001
US 2002112015	A1	15-08-2002	US UŞ	6574671 B1 2002194284 A1	03-06-2003 19-12-2002